BINARY CUBIC FORMS WITH MANY INTEGRAL POINTS

AUTHOR(S):

LIVERANCE, ERIC

CITATION:

LIVERANCE, ERIC. BINARY CUBIC FORMS WITH MANY INTEGRAL POINTS. 数理解析研究所講究録 1997, 998: 93-101

ISSUE DATE:

1997-06

URL:

http://hdl.handle.net/2433/61275

数理解析研究所講究録
998巻 1997年 93-101

BINARY CUBIC FORMS WITH MANY INTEGRAL POINTS

ERIC LIVERANCE
(prepared in collaboration with Cameron Stewart)

ABSTRACT. We make more explicit a result of Silverman's on integral points of binary cubic forms. Using the explicit 3-descent of Satgé, we show how to construct such binary cubic forms. As an application, we use Quer's elliptic curves with j-invariant 0 and rank 12 over $\mathbb{Q}$, to construct binary cubic forms which have many integral points.

INTRODUCTION

Let F be an irreducible binary form with integer coefficients and degree ≥ 3. Then for $m \in \mathbb{Z}$, the equation

$$F(U, V) = m$$

with U, V integral is known as Thue's equation. Many studies have been made of the problem of estimating the number of solutions, which we denote $N_F(m)$, and which Thue showed in 1909 must be finite. In 1935, Mahler [Ma] showed that for some constant $C > 0$ independent of m

$$N_F(m) > C(\log |m|)^{1/4}$$

for infinitely many m. In 1983, Silverman [Sil1] improved Mahler's exponent to $1/3$ in general by the following theorem.

Theorem (Silverman). *Let $F(U, V) \in \mathbb{Z}[U, V]$ be a cubic form with non-zero discriminant. Let $m_0 \in \mathbb{Z}$ be an integer such that the curve $E : F(U, V) = m_0 W^3$ has a point defined over $\mathbb{Q}$. Using that point as an origin, we may give E the structure of an elliptic curve with rank R. Then there is a constant $C > 0$ independent of m such that*

$$N_F(m) > C(\log |m|)^{R/(R+2)}$$

for infinitely many m.

To obtain the exponent $1/3$ from the theorem, Silverman uses a trick to produce twists of an arbitrary binary cubic form with rank at least one.

A natural question arising in this context is what type of elliptic curves are in the form in Silverman's theorem? Let $E_D : y^2 = x^3 + D$.

Proposition 1. *Let $F(U,V) \in \mathbb{Z}[U,V]$ be a cubic form with non-zero discriminant D and let $m \in \mathbb{Z}$. If the curve $C : mW^3 = F(U,V)$ has a rational point over $\mathbb{Q}$, then C is birationally isomorphic over $\mathbb{Q}$ to $E_{m^2D/4} : y^2 = x^3 + m^2D/4$.*

Remark 1. The existence of the automorphism $\eta : (U,V,W) \mapsto (U,V,\rho W)$, $\rho = e^{2\pi i/3}$, is enough to show that the j-invariant of C is 0, or equivalently, that C may be put in the form $y^2 = x^3 + D$. To see this, just take a point of C over some extension of $\mathbb{Q}$ with $W = 0$ as the origin. Then η is an endomorphism of order 3, i.e., an automorphism. As the ring of endomorphisms must be an order in an imaginary quadratic field, we see that the only ring of endomorphisms (over number fields) with this property is $\mathbb{Z}[\rho]$. Furthermore, the curves $y^2 = x^3 + D$ are the only elliptic curves with this endomorphism ring.

Remark 2. Note that if the choice of origin is fixed, the map η may not be an isogeny in that it may not fix the origin. In general, any algebraic map between elliptic curves is the composition of an isogeny (or endomorphism in this case) followed by translation by a point (Silverman [Sil2] III.4.4), $\eta = \tau_Q \circ \zeta$. Now, $\eta^3 = 1$ implies that

$$P = \zeta(\zeta(\zeta P + Q) + Q) + Q) = \zeta^3 P + \zeta(\zeta^2 + \zeta + 1)Q.$$

As this is true for every P, we find that ζ is a cube root of unity. Moreover, if $\zeta = 1$, then Q must be a three-torsion point. For example, consider the curve

$$C : W^3 = 2s(U^3 - 3rU^2V - 4DV^3)$$

where $s^2 = r^3 + D$ (see (6) below). If we take the rational point $(2r, 1, -2s)$ as the origin of C, then one can show that on $y^2 = x^3 - 27D$ (and under the isomorphism ψ given in (10) below), η acts as multiplication by ρ ($(x,y) \mapsto (\rho x, y)$) followed by translation by the point $S = (-3r\rho^2, 3s(2\rho + 1))$:

$$\begin{array}{ccc} C & \xrightarrow{\eta} & C \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ E' & \xrightarrow{\tau_S \circ \rho} & E' \end{array}$$

Lemma1. *If $\psi : E \to E'$ is any non-constant map between elliptic curves of degree d (i.e., a d-to-1 map) defined over $\mathbb{Q}$, then $E = E'/G$, where G is a Galois-invariant subgroup of d d-torsion points.*

Proof of Lemma. Any algebraic map ψ between elliptic curves can be written as $\psi = \tau \circ \phi$, where τ is translation on E' and ϕ is a d-isogeny. As ψ is defined over $\mathbb{Q}$, we have the relation

$$\tau \circ \phi = \psi = \psi^\sigma = \tau^\sigma \circ \phi^\sigma,$$

where σ is any Galois automorphism. Applying $-\tau^\sigma$, we have

$$-\tau^\sigma \circ \tau \circ \phi = \phi^\sigma.$$

Now if τ is translation by a point P, and we apply the above map to O, we find $P - P^\sigma = O$, or $\tau^\sigma = \tau$. This implies $\phi = \phi^\sigma$ and hence $\ker\phi = \ker\phi^\sigma$. As $\ker\phi$ is Galois invariant, it is defined over $\mathbb{Q}$. Hence, so is the dual isogeny $\hat{\phi}$ (use uniqueness of the dual isogeny with respect to $\hat{\phi} \circ \phi = [d]$). Hence C is isomorphic to $E/\ker\hat{\phi}$. $\square$

Lemma 2. *Let $E_D : y^2 = x^3 + D$. The only Galois invariant subgroup G of three 3-torsion points of E_D is $\{O, (0, \pm\sqrt{D})\}$. Hence the only elliptic curve that E_D is 3-isogenous to over $\mathbb{Q}$ is $y^2 = x^3 - 27D$.*

Proof. The 3-torsion points of E_D are

$$E_D[3] = \{O, (0, \pm\sqrt{D}), (-\rho^j \sqrt[3]{4D}, \pm\sqrt{-3D})\},$$

where $\rho = e^{2\pi i/3}$ is a cube root of unity. See Velu [Ve] to prove the second part. □

Proof of Proposition 1. Again, we note that since C has a rational point, it is an elliptic curve. We shall produce a non-constant rational map of degree 3 from C to $E_{-27m^2D/4}$. Then by the lemmas, we can conclude that C is isomorphic to $E_{729m^2D/4} \simeq E_{m^2D/4}$.

As for the degree 3 map, write explicitly

$$F(x, y) = ax^3 + byx^2 + cy^2x + dy^3.$$

Then let [Mo] H be the quadratic covariant of F

$$\begin{aligned} H(x, y) &= \begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} \end{vmatrix} = (bx + cy)^2 - (3ax + by)(cx + 3dy) \\ &= (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2 \end{aligned}$$

and let G be the cubic covariant of F given by

$$\begin{aligned} G(x, y) = \begin{vmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y} \end{vmatrix} &= (-27da^2 + 9cba - 2b^3)x^3 + (-27dba + 18c^2a - 3cb^2)yx^2 \\ &\quad + (27dca - 18db^2 + 3c^2b)y^2x + (27d^2a - 9dcb + 2c^3)y^3. \end{aligned}$$

Then we have the relation

$$(G/2)^2 = H^3 - \frac{27}{4}DF^2,$$

where D is the discriminant of F. Thus

$$x = H(U, V)/W^2; \qquad y = G(U, V)/2W^3 \tag{1}$$

gives a map from $C : mW^3 = F(U, V)$ to $E_{-27m^2D/4}$ (note that $F(U, V)/W^3 = m$). □

Satgé's Explicit 3-Descent

We use descent theory to construct binary cubic forms associated to elliptic curves of the form $y^2 = x^3 + D$. First we recall some facts about the general descent theory of elliptic curves (see [Sil2] Chapter X) and from Satgé's 2 papers on explicit 3-descent for elliptic curves with j-invariant 0 (see [Sat1],[Sat2]).

To set notation, let $E : y^2 = x^3 + D$ where D is a non-zero 6th power free integer. Then (see [Ca]) there is a 3-isogeny $\phi : E \to E'$, where $E' : y^2 = x^3 - 27D$ and also the dual isogeny $\hat{\phi} : E' \to E$ defined by

$$\hat{\phi}(x, y) = \left(\frac{x^3 - 108D}{9x^2}, \; y\frac{x^3 + 216D}{27x^3} \right).$$

Let G be the absolute Galois group of $\mathbb{Q}$. Then from the exact sequence of G-modules

$$0 \to E'[\hat{\phi}] \to E' \xrightarrow{\hat{\phi}} E \to 0,$$

we take Galois homology and from the long exact sequence, we obtain

$$(2) \qquad \begin{array}{c} 0 \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \xrightarrow{\delta} H^1(G, E'[\hat{\phi}]) \to H^1(G, E')[\hat{\phi}] \to 0 \\ P \mapsto \{\sigma \mapsto Q^\sigma - Q\}, \end{array}$$

where Q is any point satisfying $\hat{\phi}(Q) = P$ and δ is the connecting homomorphism. Now there is a bijective correspondence between cocycles in $H^1(G, E'[\hat{\phi}])$ and curves C which are twists of E' (modulo an equivalence relation) (see [Sil2] Theorem 3.6, p. 291). Satgé explicitly calculates a curve C whose class corresponds to the cocycle $\delta(P)$, $P \in E(\mathbb{Q})$ as follows.

Theorem (Satgé). *Let L be the Galois closure of the field of definition of Q. Then L contains $\mathbb{Q}(\sqrt{-27D})$ as subfield with $L/\mathbb{Q}(\sqrt{-27D})$ cyclic cubic. If $\mathbb{Q} \neq \mathbb{Q}(\sqrt{-27D})$, then $L/\mathbb{Q}$ is non-abelian of degree 6. Write $-27D = D_1 D_2^2$ with D_1 square-free. If $p(x)$ is any cubic polynomial whose splitting field is L, then $disc(p) = D_1 m^2$ for some integer m. Then the curve*

$$W^3 = (2D_2)^2 m p(U, V)$$

corresponds to the cocycle $\delta(P) = \{\sigma \mapsto Q^\sigma - Q\}$ in (2) above, where $p(U, V)$ is the homogenization of $p(x)$.

Now given a point $P = (r, s)$ on E, we can explicitly construct the curve C which corresponds to it under (2). If $Q = (u, v)$, then we must solve $\hat{\phi}(Q) = P$, or

$$\frac{u^3 - 108D}{9u^2} = r \qquad v\frac{u^3 + 216D}{27u^3} = s.$$

But the second equation gives v rationally in terms of everything else. The first equation is equivalent to

$$u^3 - 9ru^2 - 108D = 0.$$

Hence the field L in the theorem is the splitting field of the polynomial $p(x) = x^3 - 3rx^2 - 4D$, where we have absorbed a factor of 3. Now

$$\text{disc}(p) = -2^4 3^3 D(r^3 + D) = -2^4 3^3 D s^2 = -3^3 D(2^4 s^2) = D_1(D_2 2^2 s)^2.$$

Hence, by Satgé's theorem, $m = 2^2 D_2 s$ and our curve becomes

$$W^3 = 16 D_2^3 sp(U,V).$$

By absorbing cubes, we can rewrite this as

$$C : W^3 = (2s)p(U,V) = 2s(U^3 - 3rU^2V - 4DV^3).$$

Here the discriminant of the binary cubic form $F(U,V) = (2s)p(U,V)$ is

$$\operatorname{disc}(2sp(U,V)) = -108D(2s)^6.$$

If $H(U,V)$ and $G(U,V)$ are the quadratic and cubic covariants of F respectively then (as above) we have a map of C to E by

$$(3) \qquad \begin{aligned} x &= \frac{H(U,V)}{2^2 3^2 s^2 W^2} = (r^2U^2 - 32sDVU + 32rsDV^2)/W^2 \\ y &= -\frac{G(U,V)}{2^4 3^3 s^3 W^3} = -((r^3 + 2D)U^3 - 6rDVU^2 + 12r^2DV^2U + 8D^2V^3)/W^3. \end{aligned}$$

Note that this minus sign is forced on us in order that (5) below have solutions (The reason for the minus sign is from descent theory. See [Sil2] p. 292, [Ca] or [Li] and also see (11) below.). Setting $u = U/W$ and $v = V/W$, we must solve

$$(4) \qquad \frac{H(u,v)}{2^2 3^2 s^2} = r, \qquad \frac{G(u,v)}{2^4 3^3 s^3} = -s, \qquad F(u,v) = 1$$

or

$$(5) \qquad \begin{aligned} 4Drv^2 - 4Duv - r^2u^2 + r &= 0 \\ 8D^2v^3 + 12Dr^2uv^2 - 6Dru^2v + r^3u^3 + 2Du^3 + s &= 0 \\ 2s(u^3 - 3ru^2v - 4Dv^3) &= 1 \end{aligned}$$

Eliminating v in the first two equations (that is, taking the resultant with respect to v) we find that u must satisfy

$$16r^3s^6u^6 - 24r^5s^4u^4 + 8r^3s^5u^3 + 9r^7s^2u^2 - 6r^5s^3u + r^6(r^3 + 2D) = 0,$$

from which it is easy to find the root $u = -r/s$. Substituting into either of the equations above, we find $v = -1/2s$.

Proposition 2. *If $P = (r,s)$ is a point on $E(\mathbb{Q})$, $E : y^2 = x^3 + D$ then*

$$(6) \qquad C : W^3 = 2s(U^3 - 3rU^2V - 4DV^3)$$

has the rational point $(U,V,W) = (2r, 1, -2s)$. Moreover C is isomorphic over $\mathbb{Q}$ to $E' : y^2 = x^3 - 27D$.

Proof. To prove the second statement, we can use standard facts from descent theory. First note C corresponds to $\delta(P)$ under the correspondence between the Weil-Chatelet group $WC(E')$ and $H^1(G,E')$ ([Sil2] Theorem 10.3.6). By [Sil2] Proposition 10.3.3, $C(\mathbb{Q}) \neq \varnothing$ implies that $C \simeq_{\mathbb{Q}} E'$. □

Using this point and the above calculation with Silverman's theorem, we obtain the following result.

Theorem. *Suppose that $E_D : y^2 = x^3 + D$ is of rank R and that (r,s) is a point on E_D. Let $F(U,V) = 2s(U^3 - 3rU^2V - 4DV^3)$. Then there is a constant $C > 0$ independent of m such that*

$$N_F(m) > C(\log|m|)^{R/(R+2)}$$

for infinitely many m.

QUER'S CURVES

Now using Quer's curves of high rank, we can produce binary cubic forms with many integral points. To illustrate, note that Quer [Q] finds 3 curves of this form with rank 12, namely $y^2 = x^3 + D_i$ where

$$D_1 = -6533891544658786928$$
$$D_2 = -49317122354452517296$$
$$D_3 = -50586546986138596528.$$

The following points P_i are on $y^2 = x^3 + D_i$:

$$P_1 = (2109824, 1690470036)$$
$$P_2 = (3676420, 611232948)$$
$$P_3 = (3706924, 592751364).$$

By the calculations above, these correspond to the homogeneous spaces

$$C_1 : W^3 = 3380940072(U^3 - 6329472U^2V + 261355661786351477 12V^3)$$
$$C_2 : W^3 = 1222465896(U^3 - 11029260U^2V + 197268489417810069184)$$
$$C_3 : W^3 = 1185502728(U^3 - 11120772U^2V + 202346187944554386112).$$

Hence these forms satisfy the following result: for infinitely many integers m, the number of solutions to $2s(U^3 - 3rU^2V - 4DV^3) = m$ in integer U, V is greater than

$$C(\log|m|)^{6/7},$$

for some positive constant C.

THE EXPLICIT ISOMORPHISM

Either of Propositions 1 and 2 tells us that since

$$C : W^3 = 2s(U^3 - 3rU^2V - 4DV^3)$$

has the rational point $O = (U, V, W) = (2r, 1, -2s)$ and discriminant $-108D(2s)^6$, it should be isomorphic over $\mathbb{Q}$ to $E' : y^2 = x^3 - 27D$, $\psi : C \xrightarrow{\sim} E'$ (in the notation of the proposition, we have $m = 1$ and we have absorbed the 6th powers into x and y). This amounts to taking this rational point as the origin, and putting C in Weierstrass form in the standard way using the Riemann Roch Theorem (see Silverman's Proposition 3.3.1 [Sil2]). Thus we must find functions x and y whose only poles are at O and of order 2 and 3 respectively. An explicit way to obtain these functions is as follows ([ST], but see also Chapter 10 of [Mo]). We let $\hat{Z}$ be the line tangent to O, $\hat{Z} : 2sV + W = 0$. Then $\hat{Z}$ intersects C at another point $P = (r, -1, 2s)$. We let $\hat{X}$ be the line tangent to P, $\hat{X} : 3r^2U - (r^3 + 4D)V - 2sW = 0$ which meets C at a third point

$$Q = [-r(27r^6 - 108s^2r^3 + 80s^4), 27r^6 - 16s^4, 4s(27r^6 - 36s^2r^3 + 8s^4)].$$

Finally, we take $\hat{Y}$ to be any other line through O, say $\hat{Y} : sU + rW = 0$, meeting C also at the points R and S. Now note that

$$(\hat{Z}) = 2(O) + (P) - I; \qquad (\hat{X}) = 2(P) + (Q) - I; \qquad (\hat{Y}) = (O) + (R) + (S) - I,$$

where I is the formal sum of the 3 points at infinity (i.e. $W = 0$) on C. Now, if we let $\hat{x} = \frac{X}{Z}$ and $\hat{y} = \frac{Y}{Z}$, then

$$(\hat{x}) = (\hat{X}) - (\hat{Z}) = (P) + (Q) - 2(O); \qquad (\hat{y}) = (\hat{Y}) - (\hat{Z}) = (R) + (S) - (P) - (O).$$

Then using the notation of Riemann-Roch, we find that $\{1, \hat{x}, \hat{x}^2, \hat{y}, \hat{x}\hat{y}, \hat{x}\hat{y}^2\} \subset \mathcal{L}(4(O) + (P))$, but yet $\mathcal{L}(4(O) + (P))$ is a 5-dimensional space. Hence we must obtain a relation of the form

$$\hat{x}\hat{y}^2 + (a\hat{x} + b\hat{y})g = c\hat{x}^2 + d\hat{x} + e.$$

Remark. Note that if the coefficient $\hat{x}^2$ or $\hat{x}\hat{y}^2$ is zero then each function has a different order of vanishing at O, hence all would be zero. Similarly, if the coefficient of $\hat{y}$ is zero, then the coefficient of $\hat{x}\hat{y}^2$ must be as well as it is the only other function with a pole at P. Thus we find $bc \neq 0$.

This translates into a set of 9 linear equations in the unknowns a, b, c, d, e. Solving these equations, we find that

$$\begin{aligned} a &= \frac{-2r^3 + 4D}{3r^2} \\ b &= \frac{s(-r^3 + 8D)}{3r^2} \\ c &= \frac{2s^3}{9r^4} \\ d &= \frac{8s^4 + 3r^3s^2 - 9r^6}{9r^4} \\ e &= \frac{s(16s^4 + 12r^3s^2 - 27r^6)}{18r^4} \end{aligned}$$

Multiplying by $\hat{x}$ and setting $y = \hat{x}\hat{y}$ and $x = \hat{x}$, we find

$$y^2 + (ax + b)y = cx^3 + dx^2 + ex. \tag{7}$$

And now we have

$$(x) = (P) + (Q) - 2(O); \qquad (y) = (Q) + (R) + (S) - 3(O).$$

Explicitly, we have

$$x = \frac{3r^2U - (r^3 + 4D)V - 2sW}{2sV + W}; y = \frac{(sU + rW)(3r^2U - (r^3 + 4D)V - 2sW)}{(2sV + W)^2}$$

and projectively,

$$
\begin{aligned}
X &= (3r^2U - (r^3+4D)V - 2sW)(2sV+W) \\
Y &= (sU+rW)(3r^2U - (r^3+4D)V - 2sW) \\
Z &= (2sV+W)^2
\end{aligned} \tag{8}
$$

Remark. Note that this map is not regular at P or at O. One may define a map compatible with the map above which is regular at these points. To see this, merely multiply X,Y,and Z above by $\ell/\hat{X}$, where ℓ is any other line through Q. By examining divisors, one may verify that Q goes to $[0,0,1]$ and that P is the other point lying on the line $x=0$, hence P goes to

$$[0,-b,1] = [0, s(r^3-8D), 3r^2].$$

By construction, we know that O must go to $[0,1,0]$. In any case, we obtain an isomorphism of algebraic varieties.

Finally, to put (7) in the appropriate Weierstrass form, we (I) complete the square on the left; (II) scale x and y so that the lead coefficients on left and right are both equal to 1; (III) translate x to remove the x^2-term (and in this case this also removes the x-term); (IV) remove sixth powers from the constant term. In other words, if we make the substitutions

$$
\begin{aligned}
x' &= \frac{(3r)^2}{s^2}\left(cx + \frac{d+a^2/4}{3}\right) \\
y' &= \frac{(3r)^3}{s^3}c\left(y + \frac{1}{2}(ax+b)\right)
\end{aligned}
$$

then we find that

$$y'^2 = x'^3 - 27D.$$

Projectively, we find

$$
\begin{aligned}
X' &= r(2sX + (4s^2 - 3r^3)Z) \\
Y' &= 6r^2Y + (-2r^3+4D)X + (s(-r^3+8D))Z \\
Z' &= r^3Z
\end{aligned} \tag{9}
$$

where now

$$Z'Y'^2 = X'^3 - 27DZ'^3.$$

Again, we note that O goes to $[0,1,0]$, P goes to $[r(4s^2-3r^3), s(9r^3-8s^2), r^3]$ and Q goes to $[r(4s^2-3r^3), s(-r^3+8D), r^3]$.

Composing with (8) above, we find the isomorphism ψ maps $C: W^3 = 2s(U^3 - 3rU^2V - 4DV^3)$ to $E': Z'Y'^2 = X'^3 - 27DZ'^3$ by

$$
\begin{aligned}
&& X' &= 3(2sV+W)(2sU - rW) \\
(10) \qquad && Y' &= 9s(2rU(U-rV) + 4DV^2 - W^2) \\
\psi: && Z' &= (2sV+W)^2
\end{aligned}
$$

Finally, we can give an explanation for the minus sign in (4) above. This is because the following diagram is commutative.

$$\begin{array}{ccc} C & \xrightarrow{\text{descent}} & E \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\tau(r,s)} \\ E' & \xleftarrow{\hat{\phi}} & E \end{array} \tag{11}$$

Following along the left and bottom, we see that $(2r, 1, -2s)$ goes to $O \in E$. Hence the descent map (3) takes $(2r, 1, -2s)$ to $(r, -s)$.

References

[Ca] J.W.S.Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, 1992.

[Li] Eric Liverance, $x^3 + y^3 = p$, preprint.

[Ma] K. Mahler, *On the lattice points on curves of genus 1*, Proc. London Math. Soc. **39** (1935), 431-466.

[Mo] Mordell, *Diophantine Equations*, Academic Press, 1969.

[Q] Jordi Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C.R. Acad. Sci. Paris **305** (1987), 215-218.

[Sat1] Philippe Satgé, *Une généralisation du calcul de Selmer*, Séminaire de Théorie des Nombres, Paris, Birkhäuser, 1983, pp. 245-265.

[Sat2] Philippe Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory **23** (1986), 294-317.

[Sil1] Joseph H. Silverman, *Integer points on curves of genus 1*, J. London Math. Soc. **28** (1983), 1-7.

[Sil2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[ST] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer, 1992.

[Ve] J. Velu, *Isogénies entre courves elliptiques*, C. R. Acad. Sc. Paris (1971), 238-241.